DTIC FILE COPY

(2)

DTIC
ELECTE
JUN 25 1990
S D
D
Co

AD-A223 167

Yale University
Department of Computer Science

Secret Bit Transmission Using a Random Deal of Cards

Michael J. Fischer Michael S. Paterson
Charles Rackoff

YALEU/DCS/TR-792
May 1990

DISTRIBUTION STATEMENT A
Approved for public release
Distribution Unlimited

This work was supported in part by the National Science Foundation under grant number DCR-8405478 and by the Office of Naval Research under contract numbers N00014-82-K-0154 and N00014-89-J-1980. We are grateful to the Sonderforschungsbereich 124 of the Universität des Saarlandes for partial support of this research.

BEST
AVAILABLE COPY

90 06 21 018

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: TR 792
2. GOVT ACCESSION NO.:
3. RECIPIENT'S CATALOG NUMBER:

4. TITLE (and Subtitle): SECRET BIT TRANSMISSION USING A RANDOM DEAL OF CARDS
5. TYPE OF REPORT & PERIOD COVERED: Technical Report
6. PERFORMING ORG. REPORT NUMBER:

7. AUTHOR(s): Michael J. Fischer, Yale University
Michael S. Paterson, University of Warwick
Charles Rackoff, University of Toronto

8. CONTRACT OR GRANT NUMBER(s): ONR N00014-82-K-0154, ONR N00014-89-H-1980, NSF DCR-8405478

9. PERFORMING ORGANIZATION NAME AND ADDRESS: Yale University
Dept. of Computer Science
P.O. Box 2158 Yale Station
New Haven, CT 06520-2158

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS:

11. CONTROLLING OFFICE NAME AND ADDRESS:

12. REPORT DATE: May 1990
13. NUMBER OF PAGES: 8

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office): Office of Naval Research
800 North Quincy Street
Arlington, VA 22217

15. SECURITY CLASS. (of this report): unclassified
15a. DECLASSIFICATION/DOWNGRADING SCHEDULE:

16. DISTRIBUTION STATEMENT (of this Report): Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report):

18. SUPPLEMENTARY NOTES:

19. KEY WORDS (Continue on reverse side if necessary and identify by block number):

cryptography, communication, random deal, information-theoretic, distributed computing, security, protocol, multi-party, secrecy

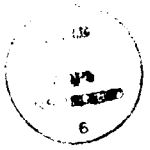
20. ABSTRACT (Continue on reverse side if necessary and identify by block number):

Protocols are developed and analyzed for transmitting a secret bit between a sender and a receiver process using only the information contained in a random deal of hands of specified sizes from a deck of n distinct cards. The sender's and receiver's algorithms are known in advance, and all conversation between sender and receiver is public and is heard by all. A correct protocol always succeeds in transmitting the secret bit, and the other player(s), who receive the remaining cards and are assumed to have unlimited computing power, gain no information whatsoever about the value of the secret bit. (CONTINUED ON REVERSE)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-LF-014-6601

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

20. (CONTINUED FROM FRONT)
In other words, their probability of correctly guessing the secret bit is exactly the same after listening to a run of the protocol as it was before. Both randomized and deterministic protocols are considered. A randomized protocol is described which works whenever the sender's and receiver's hands comprise a constant fraction of the deck, for all sufficiently large decks. A deterministic protocol is also described, but it requires the sender and receiver to each have approximately 44% of the cards. A general condition is presented that provides a lower bound on sizes of the sender's and receiver's hands in order for a protocol to exist. There is still a considerable gap between the upper and lower bounds, and improving the bounds remains an open problem.



Accesion For	
NTIS CRA&I	☑
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution /	
Availability Codes	
Dist	Avail and / or Special
A-1	

Secret Bit Transmission Using a Random Deal of Cards*

(Extended Abstract)

Michael J. Fischer
Yale University

Michael S. Paterson
University of Warwick

Charles Rackoff
University of Toronto

Abstract

Protocols are developed and analyzed for transmitting a secret bit between a sender and a receiver process using only the information contained in a random deal of hands of specified sizes from a deck of n distinct cards. The sender's and receiver's algorithms are known in advance, and all conversation between sender and receiver is public and is heard by all. A correct protocol always succeeds in transmitting the secret bit, and the other player(s), who receive the remaining cards and are assumed to have unlimited computing power, gain no information whatsoever about the value of the secret bit. In other words, their probability of correctly guessing the secret bit is exactly the same after listening to a run of the protocol as it was before. Both randomized and deterministic protocols are considered. A randomized protocol is described which works whenever the sender's and receiver's hands comprise a constant fraction of the deck, for all sufficiently large decks. A deterministic protocol is also described, but it requires the sender and receiver to each have approximately 44% of the cards. A general condition is presented that provides a lower bound on sizes of the sender's and receiver's hands in order for a protocol to exist. There is still a considerable gap between the upper and lower bounds, and improving the bounds remains an open problem.

1 Introduction

In the game of bridge, partners exchange public bids in order to arrive at a contract before playing the cards. In the course of bidding, partners gain information about each other's hands, and indeed, considerable effort has been put into designing bidding conventions (protocols in our terminology) for maximizing the amount of useful information conveyed to the partner. It is of course desirable that the opponents obtain as little useful information as possible from the bidding.

It is considered dishonest for partners to use secret conventions, and the laws of bridge require that a partnership make public their conventions prior to play. Nevertheless, one partner may well learn more from her partner's bid than do the opponents. For example, a partner responding to the Blackwood convention makes a bid whose meaning is the number of aces held. While all players thereby learn that number, the initiating partner will learn

*This work was supported in part by the National Science Foundation under grant number DCR-8405478 and by the Office of Naval Research under contract numbers N00014-82-K-0154 and N00014-89-J-1980. We are grateful to the Sonderforschungsbereich 124 of the Universitat des Saarlandes for partial support of this research.

by inference *which* aces the responding partner holds if the initiator happens to hold all of the remaining aces.

Peter Winkler carried this idea further and developed bidding conventions whereby one player could send her partner secret information about her hand that was totally unrelated to the actual bid and completely undecipherable to the opponents, even though the protocol was known to them [1, 2, 3, 4]. While one such convention was turned down in Great Britian for use in tournament play, the idea that card games could be used to achieve perfect cryptography without further assumptions remains intriguing and led to this paper.

2 Secret Bit Transmission

The secret bit transmission problem that we study is the classical problem of cryptography. An agent, Alice, has a secret bit s, which she wishes to send to another agent, Bob. All communication is via an insecure channel, so we must proceed under the assumption that an eavesdropper, Eve, overhears all communication between Alice and Bob. The goal of the protocol is for Bob to learn s but for Eve to gain no information about s. In other words, Eve's probability of correctly guessing s is unchanged after listening to the run of the protocol between Alice and Bob. Since Eve is assumed to have unlimited computing power, cryptographic systems based on computational difficulty are not applicable, and we seek instead a perfect scheme in the information-theoretic sense.

We are interested only in protocols that *always* work, as opposed to protocols that only sometimes work or that have a probability of error. Thus, we say that a protocol solves the *secret bit transmission problem* if in *every* run, Bob learns s and Eve gains no information about s.

Of course, if Alice and Bob share a random secret bit r which is not known to Eve, then it suffices for Alice to send the message $m = r \oplus s$ (the exclusive "or" of r with s). Bob computes $s = m \oplus r$, and Eve learns nothing about s, since the possibility that $s = 0$ and $r = m$ and the possibility that $s = 1$ and $r = 1 \oplus m$ are equally likely given knowledge only of m. r is called a "one-time pad" (since it cannot safely be used again to send another message), and this scheme is an example of a secure private-key cryptosystem for sending a single secret bit.

A generalization of the one-time pad is important when we consider determinstic protocols. Suppose that Alice and Bob share a random value $r \in \{0, \ldots, d-1\}$. When d is odd, r cannot be mapped to a random fair bit, but it can still be used to send s secretly, namely, Alice sends the message $m = (r + s) \bmod d$. As in the binary case, Eve learns nothing about s since all values m are equally likely, regardless of the value of s. We call such an r a *d-generalized one-time pad.*

We rule out private key cryptography by assuming that Alice and Bob have no prior secret information between themselves. Both the protocols and initial state of Alice and Bob are known to Eve. The only information that Eve does not know in advance is the value of the secret bit s, which we can regard as a private input to Alice.

It is easily shown that without any further assumptions, secret bit transmission is impossible, for Eve can simulate Bob and reach the same conclusion as to the value of s that Bob does. In case Bob is a deterministic algorithm, the simulation is obvious. If Bob is a

randomized algorithm (i.e. can flip private fair coins), then Eve simulates Bob on all possible coin-toss sequences, discarding those simulated runs in which the simulated behavior deviates from Bob's actual observed behavior. Any remaining simulated runs are *possible* runs for Bob, and thus any such run that determines a value for s must determine the correct value. In this way, Eve learns s.

Henceforth, we assume that the three players have available randomly dealt hands from a deck of n distinct totally-ordered cards. In an (a, b, c) deal, Alice gets a cards, Bob gets b cards, and Eve gets $c = n - a - b$ cards. The size of the deck, the values of the cards in the deck, and the total ordering on the cards are common knowledge among all players, as are the cardinalities of each player's hands. Only the identities of the particular cards in each player's hand are private to that player. Unlike a deal in a real card game, we assume that each player's hand is sorted by the dealer, so that no random information is contained in the order in which the cards are presented to the player. This assumption is significant when we discuss deterministic protocols.

In carrying out a secret bit transmission using a deal of cards, players are allowed to say anything they want and to reveal as much information as they like about their hands. The only requirement is that Bob eventually learns s and Eve remains in completely in the dark about s. A protocol that, given a random (a, b, c) deal, succeeds in transmitting s secretly is called an (a, b, c) *secret bit transmission protocol.*

3 A Simple Randomized Protocol

To illustrate some of the basic ideas underlying this problem, we first consider a simple randomized protocol and prove that it works whenever $a, b \geq 1$ and $a + b \geq c + 2$.

A *key set* K consists of any two cards, one from Alice's hand and one from Bob's hand. We say that $K = \{x, y\}$ is *hidden* if the two situations, that Alice holds x and Bob holds y or that Alice holds y and Bob holds x, are equally likely, given the information available to Eve. Note that by this definition, K can be hidden even though Eve knows which two cards are in K.

Assuming Alice and Bob can somehow identify a hidden key set $K = \{x, y\}$, they can then obtain from it a one-time pad r. Namely, they agree that $r = 0$ if Alice holds the smaller card in K and $r = 1$ if she holds the larger. Since Alice and Bob each know which card of K they hold, they each also know r. Eve on the other hand has no information about which card which partner holds, so r looks completely random to her. Alice can then use r to send s to Bob as described above.

The following protocol allows Alice and Bob to determine a key set:

1. Alice chooses a random card x contained in her hand and a random card y not in her hand and proposes $K = \{x, y\}$ as a key set to Bob.[1]

2. If Bob holds y (i.e. holds a card in K), he knows that K is a key set, so he *accepts* K and announces that fact to Alice, who then also knows that K is a key set. K is hidden since it is equally likely to be proposed by Alice in the symmetric deal in

[1]To keep from revealing information about which of the two cards she holds, she sorts K into increasing order before sending it to Bob.

which everything is the same except that Alice holds y and Bob holds x. K is the desired key set and the protocol terminates.

3. If Bob does not hold y, he *rejects* K and announces this fact to Alice. In this case, the facts that Alice holds x and Eve holds y are common knowledge between Alice and Eve, so Alice tells these facts to Bob as well, making the locations of x and y public. Alice and Bob then discard x and y from the deck and go back to step 1 of the protocol, pretending that the cards remaining in their hands came from a $(a-1, b, c-1)$ deal from an $n-2$ card deck. Eve has no information about how the remaining cards not in her hand are divided up between Alice and Bob, so the remaining hands indeed look random to her. Alice and Bob keep repeating the protocol in this way until they find a key set or until Alice is unable to complete step 1 (because either her hand is empty or she holds all of the cards in the deck).

If $a > c$, then Eve runs out of cards before Alice does, since both Alice and Eve lose one card on each iteration where Alice proposes a set K that is rejected by Bob. If also $b \geq 1$, then when c becomes 0, the next proposed key set is guaranteed to be accepted by Bob and the protocol terminates.

By modifying this protocol so that on each iteration, Alice and Bob switch roles if Bob holds more cards than Alice, we obtain:

Theorem 1 *Let $a, b \geq 1$ and $a + b \geq c + 2$. Then there is a randomized (a, b, c) secret bit transmission protocol.*

4 A Solution Requiring Only a Fraction of the Cards

The protocol of Section 3 requires that Alice and Bob jointly are dealt more than half the cards. We next sketch a protocol in which Alice and Bob each receive only $\lfloor \alpha n \rfloor$ of the cards, where α is an arbitrary positive constant.

The idea here is to generalize the notion of a key set. Call a set K an *i-set* if the cardinality of K is i and K contains exactly one card from each of Alice's and Bob's hands (and the remaining $i-2$ cards belong to Eve's hand). By this definition, a key set as previously defined is the same as a 2-set.

The protocol operates in two phases. The first phase produces a large collection of disjoint m-sets and $(m-1)$-sets, where $m = \lceil n/a \rceil$. A reduction phase then transforms this collection into a single 2-set. The reduction phase operates iteratively, at each stage replacing two sets in the collection by a new set. An entropy argument is used to show that the reduction process eventually terminates in a 2-set, assuming the initial collection of sets was sufficiently large.

In slightly more detail, Alice initially partitions the deck into a sets, each of which contains one card from her hand and either $m-1$ or $m-2$ cards not in her hand. Bob accepts a proposed set if he holds one or more cards in it; otherwise he rejects it. In the worst case, he will accept at least $b/(m-1)$ sets since all of his cards lie in the various proposed sets. By making n sufficiently large, the number of accepted sets can be made arbitrarily large.

If Bob holds more than one card in an accepted set, he randomly chooses one such card to keep and he discards the rest. The result is an m'-set for some $m' \leq m$. Hence, the first phase yields at least $b/(m-1)$ m'-sets of various sizes $m' \leq m$.

In the reduction phase, Alice chooses two sets R, S of maximal size from the collection. For definiteness, say R is an i-set and S is a j-set ($2 < i, j \leq m$). She then chooses one of the two sets at random, say R. Let x be the (unique) card in R that Alice holds. Let y be chosen randomly from among the cards of S that Alice does *not* hold. Alice then proposes $T = \{x, y\}$ as a key set, and Bob accepts or rejects it according to whether he holds y or not. If he accepts it, then T is a 2-set, and the reduction phase succeeds. If not, then Alice announces the locations of the cards in $R \cup \{x, y\}$ which are then discarded. She removes R and S from her collection of sets and puts the new set $S' = S - \{y\}$, which is a $(j-1)$-set, back into the collection. This process is repeated until either a key set is obtained or until only one set remains in the collection. A simple inductive proof shows that if the collection originally contains at least 2^{m-2} sets, then the reduction process eventually yields a key set.

The above establishes:

Theorem 2 *Let α be an arbitrary positive real number. There exists n_0 such that for all $n \geq n_0$, if $a = b = \lfloor \alpha n \rfloor$ and $c = n - a - b$, then there is a randomized (a, b, c) secret bit transmission protocol.*

For the above protocol, n_0 is $O(m^2 2^m)$. The protocol can be improved to yield a much smaller bound, which we currently believe will work out to about $O(m^{c \log m / \log \log m})$ for some constant c. The protocol improvements involve both phases. In phase 1, if Bob holds more than $k > 1$ cards in a proposed m'-set then, rather than discard the extras, he can partition the set into k sets each of size about m'/k such that he holds a card in each. One of them will contain Alice's card and hence be an m''-set for $m'' \approx m'/k$. In phase 2, instead of choosing two sets R and S and forming a trial 2-set T, it is better to choose r sets $R_1, \ldots, R_r$ from the collection and to form a trial r-set T by choosing one card from each R_i such that T has exactly one card from Alice's hand and $r-1$ cards not in her hand. If Bob accepts T, then T is an r-set and replaces $R_1, \ldots, R_r$ in the collection. Otherwise, the cards in T are discarded, leaving r sets $R'_i = R_i - T$, $1 \leq i \leq r$. Since T contained one card from Alice's hand, one of the R'_i sets has an empty intersection with Alice's hand, and it too is discarded. The remaining R'_j sets are returned to the collection. r is chosen at each stage to optimize the progress made. Our improved bound results from taking r approximately equal to $m \log \log m / \log m$.

5 A Lower Bound Theorem

The above protocols establish triples (a, b, c) for which an (a, b, c) secret bit transmission protocol exists. We now present a lower bound on the sizes of Alice's and Bob's hands for such a protocol to exist.

Theorem 3 *Let $n = a + b + c$. Let γ be the probability that a pair of random hands A (for Alice) and B (for Bob) intersect when dealt from* different *decks, where as usual, $|A| = a$ and $|B| = b$. If $\gamma < 1/2$, then there is no (a, b, c) secret bit transmission protocol, even if Eve is not allowed to look at her hand.*

The idea behind the proof is to look at runs of the protocol according to the transcript (conversation) τ that Eve hears. Assume for the moment that Alice and Bob are deterministic protocols, so τ is a function of s, A, and B. Call the triple (s, A, B) a *situation*. The secrecy condition implies that the number of situations giving rise to τ with $s = 0$ is the same as the number with $s = 1$. Now suppose $(0, A_0, B_0)$ and $(1, A_1, B_1)$ are two situations both giving rise to τ. Then an easy inductive argument shows that the situations $(0, A_0, B_1)$ and $(1, A_1, B_0)$ also give rise to τ. Moreover, since Bob outputs 0 in $(0, A_0, B_0)$ and outputs 1 in $(1, A_1, B_1)$, then he outputs 0 in $(1, A_1, B_0)$ and outputs 1 in $(0, A_0, B_1)$. Since his answers in these latter two situations are both incorrect and we assume a correct protocol, it must be the case that these situations cannot occur in a proper deal, i.e. $A_0 \cap B_1 \neq \emptyset$ and $A_1 \cap B_0 \neq \emptyset$. Thus, corresponding to legal pairs (A_0, B_0) and (A_1, B_1) (i.e. pairs dealt from the same deck) are illegal pairs (A_0, B_1) and (A_1, B_0). A counting argument shows that # legal pairs $\leq$ # illegal pairs, from which it follows that $\gamma \geq 1/2$. Hence, if $\gamma < 1/2$, then no protocol exists.

When Alice and Bob are randomized algorithms, the transcript τ depends on Alice's and Bob's random choice sequences as well as on s, A, and B, so the definition of a situation must be extended to include the choice sequences, and one must sum over all choice sequences at the end. Details are given in the full paper.

Corollary 1 *There is no* $(1, 1, 1)$ *secret bit transmission protocol.*

Proof: For this case, $\gamma = 1/3 < 1/2$. ■

6 Deterministic Protocols

The protocols given so far in this paper heavily exploit randomization by the players. Moreover, it is not at all clear how to get rid of randomization. For example, if Alice proposes a key set $\{x, y\}$ by picking the *smallest* card in her hand for x and the *smallest* card not in her hand for y, then she may be revealing her entire hand by announcing the set $\{x, y\}$. For example, if $a < n/2$ and the set she announces contains card number $n - a + 1$, that card must be x, and Alice's hand is $\{n - a + 1, n - a + 2, \ldots, n\}$, where as usual, $n = a + b + c$, and we assume the cards of the deck are numbered $1, 2, \ldots, n$. Nevertheless, deterministic protocols are possible, at least for some triples of hand sizes. We describe a recursive protocol below.

The protocol proceeds as follows on an (a, b, c) deal:

1. If $a, b \geq 1$ and $c = 0$, then there are $d = \binom{n}{a}$ possible $(a, b, 0)$ deals. Index them from 0 to $d - 1$ in some predetermined way, and let r be the index of the actual deal. Both Alice and Bob know the exact placement of every card (since $c = 0$), so both can compute r. Eve however has no information about r. Alice sends s to Bob using r as a d-generalized one-time pad as described in Section 1, and the protocol succeeds.

2. If $a = 0$ or $b = 0$, there is nothing Alice or Bob can do and the protocol fails.

3. If n is odd, Alice and Bob determine the location of card n by each announcing whether or not they hold the card, and that card is discarded from further play. This

leaves the three players with a random deal from a deck of $n-1$ cards and hands of sizes $(a-1,b,c)$, $(a,b-1,c)$, or $(a,b,c-1)$, depending on which of the three players originally held card n. Alice and Bob know which of these three situations they are in, and they play accordingly by using this protocol recursively.

4. If n is even, Alice and Bob regard the deck as consisting of $n/2$ *suits* of two cards each by mapping card $2k$ to suit k, rank 0, and card $2k+1$ to suit k, rank 1. Alice and Bob then name all of their singleton suits. If they both name the same singleton suit, then the two cards of that suit form a key set and the protocol succeeds. If not, then Eve holds the other card of each singleton suit named by either Alice or Bob.

   Alice and Bob now select a subset of the deck for which they have a random deal and they use this protocol recursively on the subset. The subset consists of all cards of rank 0 and all suits k such that k is *not* one of the singleton suits named by either Alice or Bob. Let (a',b',c') be the numbers of cards in the subset held by Alice, Bob, and Eve, respectively. If Alice previously named p singleton suits and Bob named q, then $a'=(a-p)/2$, $b'=(b-q)/2$, and $c'=(c-p-q)/2$. This is because after all of the cards of singleton suits have been discarded, then every player that holds the rank 0 card of a suit also holds the rank 1 card of the same suit.

This protocol always succeeds for (a,b,c) if either $a,b\geq 1$ and $c=0$, or if it always succeeds on all of the smaller deals that might be produced by the above rules. The recurrence relation that results is not particularly well-behaved, but we can prove the following:

Theorem 4 *There exists a deterministic (a,b,c) protocol for secret bit transmission if $a,b\geq 1$ and $c\leq \min(a,b)/3$.*

7 Conclusion and Open Problems

This work is a first step at trying to understand the notion of the shared secret random information contained in a deal of cards and to find protocols to make use of such shared information. It also gives further insight into the power of private coins and multiround interaction.

An obvious direction for further investigation is to find tighter bounds on triples (a,b,c) for which randomized and deterministic (a,b,c) protocols do and do not exist. An obvious extension is to consider the problem of sending more than one secret bit with a single deal of cards and/or to relax some of the requirements we have imposed on a solution. For example, one might allow a small probability of error in the protocol so that Bob sometimes fails to learn the secret, or Eve sometimes does learn the secret, or Eve's probability of correctly guessing the secret increases by a small positive ϵ.

Another direction for further research, suggested by Peter Winkler, is to replace probabilistic statements by knowledge statements. Thus, the problem becomes one of finding an (a,b,c) protocol such that after running it, Bob knows the secret value but Eve does not. Every secret bit transmission protocol satisfies these conditions, but the converse does not hold, for even when Eve does not learn the secret bit for sure, she may nevertheless have acquired partial information about it. Our lower bound theorem does not seem to

apply to this case, and it appears that a detailed analysis of the knowledge structure will be necessary.

A final avenue for further research is to look at even more restricted protocols. For example, a *one-way deterministic protocol* is one in which Alice sends only a single message to Bob, who then, on the basis of his hand, can figure out Alice's secret but Eve learns nothing about it. Andrew Berman has shown that such protocols can exist by exhibiting one for a $(5, 4, 1)$ deal. It is an open problem to find other non-trivial triples for which such one-way protocols exist.

Acknowledgement

We are grateful to Andrew Berman for helpful discussions.

References

[1] Jeremy Flint. Cheating by degrees. *The Times Saturday Review*, May 1981.

[2] Peter Winkler. Cryptologic techniques in bidding and defense, parts i, ii, iii, and iv. *Bridge Magazine*, April: 148–149, May: 186–187, June: 226–227, and July: 12–13, 1981.

[3] Peter Winkler. My night at the cryppie club. *Bridge Magazine*, pages 60–63, August 1981.

[4] Peter Winkler. The advent of cryptology in the game of bridge. *Cryptologia*, 7(4):327–332, October 1983.